PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-007288
(43)Date of publication of application : 11.01.2002

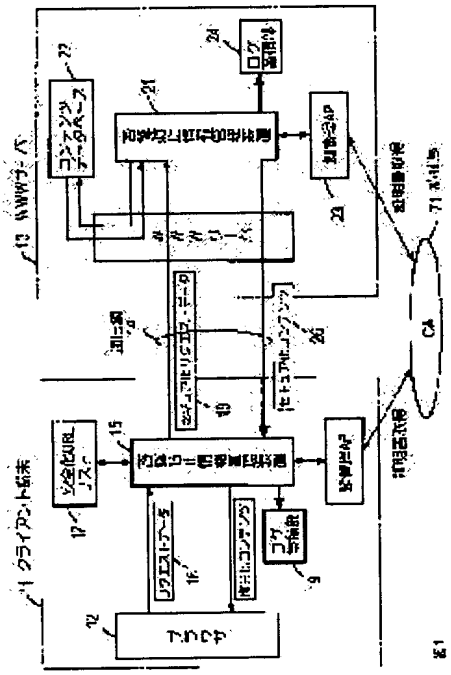
(51)Int.CI. G06F 13/00
G06F 12/14
G06F 15/00
G09C 1/00
H04L 9/32

(21)Application number : 2000-186279
(22)Date of filing : 21.06.2000

(71)Applicant : NTT COMMUNICATIONS KK
(72)Inventor : YASUDA HITOSHI
WATANABE TORU
OGIWARA TOSHIHIKO
TABUCHI HIROYASU

(54) METHOD AND DEVICE FOR MANAGING NEGATION PREVENTION INFORMATION, AND PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To store a log of transmitted or received information in a safe state such that it cannot be negated later.
SOLUTION: A browser 12 sends out a GET Request 16, and then when acquisition in a secured state is desired, a managing device 18 detects of this by a secure URL list 17, adds key information on a client in it to the Request 16, and sends them to a server 12. The server 12 extracts contents corresponding to the Request, and the managing device 21 gives a signature thereto, ciphers the contents with the open key of the client based upon the key information, and stores the ciphered contents in a log 24 and also sends them in client MOSS format, while indicating that the data are ciphered data in its header. The managing device 15 stores the ciphered contents in a log 19 and then deciphers the contents.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－7288
（P2002－7288A）
(43)公開日　平成14年１月11日(2002.1.11)

(51)Int.Cl.[7]		識別記号	FI			テーマコード（参考）
Ｇ０６Ｆ	13/00	６１０	Ｇ０６Ｆ	13/00	６１０Ｓ	５Ｂ０１７
	12/14	３２０		12/14	３２０Ａ	５Ｂ０８５
	15/00	３３０		15/00	３３０Ａ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ	
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｄ	

審査請求　未請求　請求項の数18　ＯＬ　（全 13 頁）

(21)出願番号　特願2000－186279(P2000－186279)

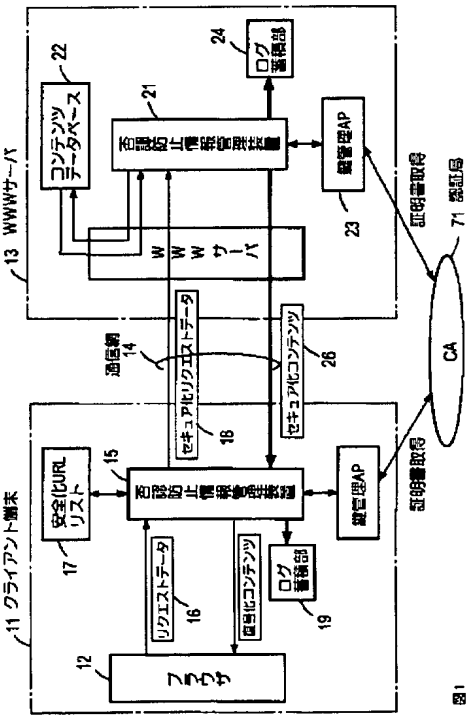
(22)出願日　平成12年６月21日(2000.6.21)

(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　安田　仁
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

最終頁に続く

(54)【発明の名称】　否認防止情報管理方法、その装置及びプログラム記録媒体

(57)【要約】
【課題】　送信情報又は受信情報について、後で否認できないように安全な状態でそのログを蓄積する。
【解決手段】　ブラウザ１２からＧＥＴ　Ｒｅｑｕｅｓｔ１６を送出すると、それがセキュア状態での取得をしたい場合は、管理装置１９でこのことをセキュアＵＲＬリスト１７で検出し、そこにあるクライアントの鍵情報をＲｅｑｕｅｓｔ１６に追加してサーバ１２へ送る、サーバ１２はＲｅｑｕｅｓｔに応じたコンテンツを取出し、管理装置２１でこれに対し、署名を付け、前記鍵情報にもとづくクライアントの公開鍵で暗号化し、この暗号化コンテンツをログ２４に蓄積すると共にクライアントＭＯＳＳフォーマットでそのヘッダに暗号化データであることを示して送信する。管理装置１５ではその暗号化コンテンツをログ１９に蓄積した後、復号する。



1

【特許請求の範囲】

【請求項１】　アプリケーションデータに対し、送信者の電子署名を行い、
その署名付アプリケーションデータをログ蓄積部に蓄積すると共に相手方へ送信することを特徴とする否認防止情報管理方法。

【請求項２】　上記署名付アプリケーションデータをログ蓄積部に蓄積するに先立ち、暗号化して上記蓄積を行うと共に相手方へ送信することを特徴とする請求項１記載の否認防止情報管理方法。

【請求項３】　受信した署名付アプリケーションデータをログ蓄積部に蓄積し、
上記受信した署名付アプリケーションデータに対し、その署名の検証を行い、その検証に合格すると、上記署名付アプリケーションデータを真として処理することを特徴とする請求項１記載の否認防止情報管理方法。

【請求項４】　上記受信した署名付アプリケーションデータは暗号化されたものであり、
その暗号化された署名付アプリケーションデータを上記ログ蓄積部に蓄積し、
上記暗号化された署名付アプリケーションデータを復号し、その復号した署名付アプリケーションデータに対して上記署名検証を行うことを特徴とする請求項１又は２記載の否認防止情報管理方法。

【請求項５】　上記送信アプリケーションデータはブラウザから出力されたものであり、
それがＧＥＴかＰＯＳＴか判定し、
ＰＯＳＴであれば上記暗号化の鍵を、サーバからブラウザに送られた鍵情報にもとづき取得し、
上記ブラウザからの出力がＧＥＴであれば、上記アプリケーションデータに対し署名、暗号化をすることなく、送信者の鍵情報を追加して送信することを特徴とする請求項１乃至４の何れかに記載の否認防止情報管理方法。

【請求項６】　先ず安全化条件を満たすかを判断し、安全化条件を満すと、上記電子署名とそれ以後の処理を行い、安全化条件を満たさないと、上記アプリケーションデータを上記ログ蓄積部に蓄積することなく、そのまま送信することを特徴とする請求項１乃至５の何れかに記載の否認防止情報管理方法。

【請求項７】　クライアント端末からの鍵情報はアプリケーションデータを受信し、
その受信したアプリケーションデータに付加された鍵情報を一時保存し、
上記受信したアプリケーションに応じたコンテンツを含むアプリケーションに対し、電子署名を行い、
その署名付アプリケーションを上記保存した鍵情報にもとづき暗号化し、
その暗号化アプリケーションデータをログ蓄積部に蓄積すると共に上記クライアント端末へ送信することを特徴とする否認防止情報管理方法。

2

【請求項８】　クライアント端末からの鍵情報付アプリケーションデータを受信し、
その受信したアプリケーションデータに付加された鍵情報を一時保存し、
上記受信したアプリケーションに応じた、署名付コンテンツを含むアプリケーションを上記保存した鍵情報にもとづき暗号化し、
その暗号化アプリケーションデータをログ蓄積部に蓄積すると共に上記クライアント端末へ送信することを特徴とする否認防止情報管理方法。

【請求項９】　クライアント端末からの鍵情報付暗号化されたアプリケーションデータを受信し、
その暗号化されたアプリケーションデータをログ蓄積部に蓄積し、
かつ上記アプリケーションデータに付加された鍵情報を一時保存し、
上記暗号化されたアプリケーションデータを復号し、
その復号されたアプリケーションデータの署名を検証し、
その検証に合格すると、上記アプリケーションデータにもとづき、上記クライアント端末へ送信するアプリケーションデータが安全化の条件を満すか否かを判断し、
その条件を満たさなければ、そのままそのアプリケーションデータを送信し、条件を満せば、そのアプリケーションデータに対し電子署名を行い、その署名付アプリケーションデータを上記一時保存した鍵情報にもとづき暗号化し、その暗号化されたアプリケーションデータをログ蓄積部に蓄積すると共に送信することを特徴とする否認防止情報管理方法。

【請求項１０】　受信した署名付アプリケーションデータをログ蓄積部に蓄積し、
上記署名付アプリケーションデータに対し、その署名の検証を行い、
その検証に合格すると、上記署名付アプリケーションデータを真として処理することを特徴とする否認防止情報管理方法。

【請求項１１】　上記受信した署名付アプリケーションデータは暗号化された署名付アプリケーションデータであり、
上記ログ蓄積部への蓄積は上記暗号化された署名付アプリケーションデータに対し行い、
上記暗号化された署名付アプリケーションデータに対し復号を行い、その復号された署名付アプリケーションデータに対し、上記署名の検証を行うことを特徴とする請求項１０記載の否認防止情報管理方法。

【請求項１２】　請求項１乃至１１の何れかの方法をコンピュータに実行させるプログラムを記録した記録媒体。

【請求項１３】　アプリケーションプログラムにより動作するアプリケーション手段と、通信路との間に設けら

れる否認防止情報管理装置であって、
通信路より受信した暗号化アプリケーションデータが蓄積されるログ蓄積部と、
上記暗号化アプリケーションデータを復号する復号部と、
上記復号されたアプリケーションデータの署名を検証する検証部と、
上記検証部の検証に合格したアプリケーションデータを上記アプリケーション手段へ送る手段と、
を具備する否認防止情報管理装置。

【請求項１４】　アプリケーション手段から受け取ったアプリケーションデータに対し電子署名を行う署名部と、
上記署名付アプリケーションデータを送信先の鍵情報にもとづき暗号化する暗号部と、
上記暗号化されたアプリケーションデータが蓄積されるログ蓄積部と、
上記蓄積された暗号化されたアプリケーションデータを通信路へ送信する手段と
を備えることを特徴とする請求項１３記載の否認防止情報管理装置。

【請求項１５】　アプリケーションプログラムにより動作するアプリケーション手段と通信路との間に設けられる否認防止情報管理装置であって、
上記アプリケーション手段から受け取ったアプリケーションデータに対し電子署名を行う署名部と、
上記署名付アプリケーションデータを送信先の鍵情報にもとづき暗号化する暗号部と、
上記暗号化されたアプリケーションデータが蓄積されるログ蓄積部と、
上記蓄積された暗号化されたアプリケーションデータを通信路へ送信する手段とを具備する否認防止情報管理装置。

【請求項１６】　上記アプリケーション手段からのアプリケーションデータが安全化条件を満すか否か判定する判定手段と、その判定手段が条件を満すと判定すると上記アプリケーションデータを上記署名部へ送り、条件を満たさないと判定すると上記アプリケーションデータを上記送信手段へ送る手段とを備えることを特徴とする請求項１４又は１５記載の否認防止情報管理装置。

【請求項１７】　クライアント端末からの要求に応じてコンテンツをクライアント端末へ送信するサーバに設けられる否認防止情報管理装置において、
上記クライアント端末から受信したアプリケーションデータ中の鍵情報が一時保存される保存部と、
アプリケーションデータに対し電子署名を行う署名部と、
上記署名付アプリケーションデータを上記保存部の鍵情報にもとづき暗号化する暗号部と、
上記暗号化されたアプリケーションデータが蓄積されるログ蓄積部と、

上記ログ蓄積部に蓄積された暗号化されたアプリケーションデータを上記クライアント端末へ送信する手段とを具備する否認防止情報管理装置。

【請求項１８】　上記クライアント端末から受信したアプリケーションデータは暗号化されたものであり、
その受信暗号化アプリケーションデータが蓄積されるログ蓄積部と、
上記受信暗号化アプリケーションデータを復号する復号部と、
上記復号されたアプリケーションデータの署名を検証する検証部とを具備することを特徴とする請求項１４記載の否認防止情報管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明はクライアント端末におけるＷＷＷブラウザとＷＷＷサーバとの通信や電子メールなどにおいて、通信内容を、後で否認するおそれがある情報を、否認できないように管理する方法、その装置及びプログラム記録媒体に関する。

【０００２】

【従来の技術】例えば図１３に示すようにインターネットを介して、クライアント端末上のＷＷＷブラウザによりＨＴＭＬで記述されたテキストを解釈して表示し、希望するファイルやサービスなどをＵＲＬ（資源指定する手法）により指定して、ＨＴＴＰプロトコルによりＷＷＷサーバと通信して、ＷＷＷサーバより所望の例えばコンテンツを取得することが行われている。この場合、誰が何を注文したかのプライバシイの保護や送信中のコンテンツが盗まれてもそのコンテンツを利用できないようにする点などから、ＳＳＬ（Ｓｅｃｕｒｅｄ　Ｓｏｋｅｔｓ　Ｌａｙｅｒ）と云われる暗号ソフトウエアで暗号化して通信することが行われている。

【０００３】

【発明が解決しようとする課題】例えばクライアントが注文したコンテンツと異なるコンテンツが送られて来たとサーバに不平を云うようなことがある。この場合、クライアント端末側で注文に関するデータやサーバ側で送信コンテンツに関するデータをログとして記録保存しておいても、これらは容易に改ざんすることができるため相手を納得させることができない。つまり、そのようなデータを見せても、そのデータは否認されても仕方ないものである。

【０００４】ＳＳＬによる暗号化は、通信路上でのみ暗号化するものであり、送信先が決れば、送信情報を順次暗号化して、送信し受信側でも、受信信号を直ちに復号して始めてアプリケーションプログラムで解釈することができるものである。従って、従来のＳＳＬにより暗号化された通信路上のデータをログとして保存しておいても、どのクライアント端末又はどのサーバよりのどの通

信データであるかを区別することができない。従って、この通信路上の暗号化通信データを単にログとして保存しておいても、否認防止情報として管理することができず、つまり否認防止情報として用いることはできない。

【０００５】

【課題を解決するための手段】この発明によれば、アプリケーションデータ、つまりアプリケーションプログラムが認識できる一塊りのデータごとに署名を付け、必要に応じ暗号化して送信すると共にその署名付アプリケーションデータをログ蓄積部に蓄積しておく。また受信の際に署名付アプリケーションデータをまずログ蓄積部に蓄積し、その後、暗号化アプリケーションデータの場合は復号した後署名検証する。つまりログ蓄積部には一塊りのアプリケーションデータごとに署名が付けられており、アプリケーションプログラムで発信者（端末又はサーバ）、受信者（端末又はサーバ）の区別ができ、必要に応じて日時を付けておけば、後に問題になった時に、対応するアプリケーションデータを取出して署名を検証することにより、そのデータについて否認できないようにすることができる。

【０００６】

【発明の実施の形態】この発明をクライアント端末上のWWWブラウザとWWWサーバとの間における通信に適用した実施例を先ず説明する。図１はクライアント端末１１がそのWWWブラウザ１２により、WWWサーバ１３からインターネットなどの通信網１４を介してコンテンツを取得する場合である。ブラウザ１２と通信網１４の通信路との間にこの発明による否認防止情報管理装置１５が設けられる。

【０００７】利用者はブラウザ上の画面を見て希望するコンテンツのＵＲＬをキーボードにより入力し、又は画面上でマーカを指示させてクリックすると、ブラウザ１２からアプリケーションデータとしてリクエスト（Ｒｅｑｕｅｓｔ）データ１６が否認防止情報管理装置１５に入力される。このリクエストデータ１６は例えば図２Ａに示すように、コンテンツ取得を示すＧＥＴ、通信プロトコルｈｔｔｐ、着信アドレス、プログラムのファイル名そのプログラムに対する命令、この例ではファイル名ｍｏｓｓ．ｃｇｉ中のコンテンツｈｔｍを安全な状態で取得することを示しており、更に通信プロトコルとそのバージョン番号、プロキシイ（代理サーバ）の使用可能、サーバのソフト名などが記述されている。

【０００８】否認防止情報管理装置１５では図３に示すように、ブラウザ１２よりのリクエストデータ１６は安全化判定部３１に入力されて、コンテンツを安全に、つまり改ざんされたり、盗まれたりしない状態で取得することを要求するか否かの判断が行われる。この例ではセキュア状態で取得する安全化ＵＲＬリスト１７を設け、リクエストデータ１６中の取得ファイル名がそのリスト１７中にあれば、セキュア用リクエストとする。

【０００９】安全化ＵＲＬリスト１７は例えば図２Ｂに示すように、安全化されるべき各ＵＲＬが、ＵＲＬとクライアント名とＣＡ名と鍵番号とを順次「，」で区切られて１行としてそれぞれ記憶されている。ＣＡ名はそのクライアント名のクライアントがそのコンテンツ取得のために用いる秘密鍵に対する公開鍵を登録している認証局名であり、鍵番号（Ｋｅｙｓｅｌ）はその複数の登録公開鍵の１つを特定するための番号である。図２Ｂ中のＵＲＬの２行目において「＊」印はその前の情報はどのようなものでもよいことを示す。

【００１０】図２Ａに示した例のリクエストデータ１６中のファイル名は「ｍｏｓｓ．ｃｇｉ」であり、安全化ＵＲＬリスト１７中の２番目に該当する。よって安全化判定部３１は安全化要求をすると判定し、更に取得か否か判断部３２ではリクエストデータ１６が「ＧＥＴ」であり取得と判断し、鍵情報付加部３３でリクエストデータ１６に、安全化ＵＲＬリスト１７の該当するＵＲＬの格納部から得た鍵情報を付加して図２Ｃに示すようなセキュア用リクエストデータ１８とする。図２Ｃ中の破線より下の部分が付加された鍵情報１８ａであり、一行目が認証局ＣＡに登録されているクライアントのＥメールアドレスであり、２行目が認証局ＣＡの識別情報であり、３番目が使用する鍵番号である。このセキュア用リクエストデータ１８が通信路へ送信部３４を通じて送信される。この通信プロトコルはこの例ではＨＴＴＰである。

【００１１】サーバ１３はＨＴＴＰで受信する受信部５１（図４）で受信され、否認防止情報管理装置２１へ供給され、その受信電文がセキュア用か否かの判定が判定部５２で行われる。この判定はその電文のヘッダに付けられている後のデータの種類を表わすＭＩＭＥ　Ｃｏｎｔｅｎｔ　Ｔｙｐｅから行う。セキュア用電文であれば、安全化情報分離部５３において、ＧＥＴであれば、前記例ではセキュア用リクエストデータ１８はＧＥＴであるからその鍵情報１８ａが保存部５４に保存され、残りのデータはアプリケーション手段５５に供給される。

【００１２】アプリケーション手段５５は、サーバ１３のWWWブラウザに対する主要なアプリケーションプログラムを機能させるものである。つまりこの例では、受信したリクエストデータ１８中の「ｍｏｓｓ．ｃｇｉ？ｕｒｌ＝／ｓｅｃｕｒｅ．ｈｔｍ」にもとづきコンテンツデータベース２２からｈｔｍのコンテンツを取出し、アプリケーションデータとされたコンテンツが否認防止情報管理装置２１に供給される。

【００１３】否認防止情報管理装置２１では図４に示すように、そのアプリケーションデータとされたコンテンツは安定化されるべきであるかの判定が判定化部５６で行われる。この例ではセキュア用リクエストデータ１８中の「ｓｅｃｕｒｅ．ｈｔｍ」の「ｍｏｓｓ．ｃｇｉ」により安全化することが要求されている。従ってコンテ

ンツは署名部５７で鍵記憶部５８中のサーバ署名用鍵により電子署名が付けられ、この署名付コンテンツは暗号部５９で保存部５４に保存された鍵情報にもとづき暗号化される。つまり鍵取得部６１が鍵管理アプリケーションプログラム２３を、保存部５４の鍵情報１８ａについて実行して、そのＣＡＩＤ情報の認証局装置２４をアクセスして、鍵情報１８ａ中のクライアントＥメールアドレスと鍵番号を送り、認証局装置７１からそのクライアントのその鍵番号の公開鍵証明書を取得する。

【００１４】その取得した公開鍵証明書中の公開鍵により暗号部５９で署名付コンテンツを暗号化する。この暗号化コンテンツ（暗号化アプリケーションデータ）をログ蓄積部２４に必要に応じてその日時と共に蓄積すると共にその暗号化コンテンツは送信部６２よりＨＴＴＰプロトコルにより通信路へ送信される。このセキュア化コンテンツ２５は例えば暗号化データの国際規格フォーマットであるＭＯＳＳにフォーマット化されてあり、そのヘッダに、後のデータの種類を表わすＭＩＭＥＣｏｎｔｅｎｔ　Ｔｙｐｅに暗号化されている記述をする。なおクライアント端末１１で署名の検証ができるように、署名部５７の署名に用いた署名鍵と対応する検証用公開鍵を登録してある認証局識別情報ＣＡＩＤと、その認証局に登録してあるサーバ１３のアドレスと、署名に用いた鍵の番号（Ｋｅｙｓｅｌ）とよりなる鍵情報も、セキュア化コンテンツ２６にそのＭＯＳＳフォーマットに従った箇所に記述しておく。

【００１５】クライアント端末１１ではサーバ１３から送信されたセキュア化コンテンツ２６は否認防止情報管理装置１５の受信部３５（図３）で受信され、安全化情報分離部３６でそのヘッダのＭＩＭＥ　Ｃｏｎｔｅｎｔ　Ｔｙｐｅから暗号化データであると判定して受信セキュア化コンテンツ２６をログ蓄積部１９に必要に応じて日時と共に蓄積すると共に復号部３７で、先にセキュア用リクエストデータ１８で送った鍵情報１８ａと対応する秘密鍵を鍵記憶部３８から取出して復号する。その復号されたコンテンツを検証部３９で署名の検証を行う。この検証用鍵は、受信したセキュア化コンテンツ２６中の鍵情報を用いて、鍵取得部４１が鍵管理アプリケーションプログラムを実行して登録認証局から登録サーバアドレスの鍵番号の公開鍵証明書を取得して得る。

【００１６】その検証に合格すると復号されたコンテンツはＨＴＭＬ記述状態でブラウザ１２へ供給され、例えば画面表示される。次にブラウザ１２からのリクエストがＰＯＳＴの場合でセキュア化リクエストデータとしてサーバ１３へ送信する例を図５を参照して説明する。この場合ブラウザ１２には図６Ａに示すフォームデータ７２がサーバ１３から与えられており、そのうちのデータ７２ａはサーバ１３の認証局ＣＡに登録したアドレス、登録した認証局の識別情報ＣＡＩＤ、使用する鍵番号（Ｋｅｙｓｅｌ）よりなる鍵情報であり、これは画面に表示されない。データ７２ｂは入力された名前を表示する箇所、実行ボタン、リセットボタンが画面に表示されている。名前、図示例では「ｈｏｇｅｈｏｇｅｌ」を入力して実行ボタンを操作すると、例えば図６Ｂに示すリクエストデータ７３がブラウザ１２から否認防止情報管理装置１５へ供給される。リクエストデータ７３は図２Ａに示したリクエストデータ１６に対し、ＧＥＴがＰＯＳＴに変更され、フォームデータとして付加され、つまり図６Ａ中のサーバの鍵情報と、入力された名前などが加わった点以外はほぼ同様である。

【００１７】このＰＯＳＴリクエストデータ７３も図３の否認防止情報管理装置１５内の安全化判定部３１で安全化条件部１７の安全化ＵＲＬリスト内のＵＲＬと一致するか否かにより安全化処理を行うかの判定がなされ、この例では「ｍｏｓｓ．ｃｇｉ」により安全化処理が行われる。ＰＯＳＴリクエストデータ７３は署名部４２において、鍵記憶部３８内のクライアントの署名鍵により電子署名が付けられ、その署名付ＰＯＳＴリクエストデータは暗号部４３で、そのデータ７３内のサーバ１３の鍵情報にもとづき暗号化される。詳しくは先に述べた場合と同様にその鍵情報に基づき、鍵取得部４１によりサーバ１３の公開鍵証明書を認証局７１から取得してその公開鍵により暗号化する。このようにして得られた暗号部４３よりのセキュア化リクエストデータ７４は送信部３４により通信路へ送信される。このデータ７４の内容は例えば図６Ｃに示すようなものである。

【００１８】このセキュア化リクエストデータ７４はサーバ１３の否認防止情報管理装置２１内のＨＴＴＰ受信プログラム処理部、つまり図４の受信部５１に受信され、そのセキュア用電文判定部５２でセキュア用電文と判定され、更に安全化情報分離部５３で暗号化されたＰＯＳＴリクエストデータと判断されて、ログ蓄積部２４に日時データと共に蓄積される。またこのセキュア化リクエストデータ７４は復号部６３で鍵記憶部５８内のブラウザ１２へ送ったサーバ鍵情報と対応する秘密鍵で復号し、その復号されたＰＯＳＴリクエストデータの署名の検証を検証部６４で行う。なおこの検証が可能なように、セキュア化リクエストデータ７４内のＭＯＳＳ化フォームデータ内に、クライアント端末１１内の署名部４２の署名に用いた鍵と対応する公開鍵を得るための鍵情報が記述されてあり、この鍵情報を用いて、認証局から対応する公開鍵証明書を取得し、その公開鍵を用いて検証を行う。

【００１９】この検証に合格すると、その復号されたＰＯＳＴリクエストデータをアプリケーション手段５５、つまりＷＷＷサーバのプログラムの対応する処理部分により処理させる。このリクエストデータが例えば単なる名前の登録の場合は、その登録を行うと共にその受信したことを示すメッセージを、暗号化することなく送信部６２を通じてクライアント端末１１へ送信する。あるい

は見積書にＰＯＳＴリクエストデータ中の名前を記入して、クライアント端末１１に返送する。この際に、この内容の見積書を送ったことをクライアント端末１１のクライアントが否認できないようにするには、先のコンテンツのクライアント端末１１への送信と同様に電子署名を付け、更に暗号化し、その暗号化した回答書をログ蓄積部２４に蓄積すると共にクライアント端末１１へ送信する。

【００２０】上述において、コンテンツデータベース２２に格納されているコンテンツに対し、署名部５７によりサーバ１３の電子署名を付けておき、その署名付コンテンツをデータベース２２に格納しておいてもよい。この場合は、コンテンツをクライアント端末１１へ送信する。更に署名部５７による署名処理が省略でき、それだけ全体としての処理を高速化することができる。クライアント端末１１、サーバ１３の何れにおいても送信電文を蓄積するログ蓄積部と、受信電文を蓄積するログ蓄積部とを分離して設けてもよい。

【００２１】以上述べたように、コンテンツなどの一塊りのアプリケーションデータごとに署名を付けて、暗号化してログ蓄積部に蓄積することができる。よって、必要に応じて所望のアプリケーションデータをログ蓄積部から取出して署名検証により、その情報を署名者が否認することを不可能にすることができる。またこの実施例のように暗号化する場合は、その鍵情報からどこへ送信したかの否認も不可能とすることができる。なお例えば利用者からのログ蓄積部に蓄積したログを確認したい要求があれば、そのログをＭＩＭＥ　Ｃｏｎｔｅｎｔ　Ｔｙｐｅの次のアドレスと、ログ蓄積を行った日付から、ログ蓄積部を検索して、そのログを表示画面に表示する。これによりそのアドレスと日付から、そのログ（アプリケーションデータ）をその利用者がそのアドレスに送ったか否か、又はその利用者が受け取ったか否かを確認し、更に必要に応じてそのログ（アプリケーションデータ）を復号部に復号させ、その復号結果に対する署名を検証部に行わせ、その検証結果の表示を見て、例えば不合格ならそのログは誤りがあるものとして削除したり、合格を確認して利用者が満足すれば、そのログの確認処理を終了する。更に必要に応じてそのログのアプリケーションデータの内容も確認したい要求があれば、先に復号したログを呼び出して表示画面に表示する。なお管理者は古くなり不要となったログの削除なども行う。

【００２２】クライアント端末１１は例えばパーソナルコンピュータにより構成され、その場合、例えば図７に示すように、安全化ＵＲＬリストメモリ１７、ログ蓄積部１９、鍵記憶部３３、送信部３４、受信部３５、ブラウザプログラムが記憶されたメモリ８１、否認防止情報管理プログラムが記憶されたメモリ８２、鍵管理プログラムが記憶されたメモリ８３、コンピュータの基本動作を行う基本プログラムが記憶されたメモリ８４、ＣＰＵ８５がバス８６に接続されて、全体としての機能が行われる。なおメモリ８１，８２，８３に対しては対応するプログラムが、外部から予めインストールされるが、対応したプログラムが格納されたものを直接接続してもよい。更に否認防止情報管理プログラムの実行において、署名処理、暗号化処理、復号化処理、検証処理などソフトウエアで行うことなく、モジュール化された復号部３７、検証部３９、署名部４２、暗号部４３を利用するようにしてもよい。これらモジュール化したものの利用はその全てに限らず、そのうちのいくつかを行ってもよい。図に示さないがサーバ１３も同様にコンピュータを用いた構成とすることができる。

【００２３】クライアント端末１１側の否認防止情報管理装置１５の動作処理の手順は図８に示すようになる。ブラウザ１２からリクエストを受信すると（Ｓ１）、そのリクエストが安全化（セキュア）条件に該当するかを調べ（Ｓ２）、該当しない場合はそのままサーバ１３へ送信し（Ｓ３）、該当する場合はそのリクエストがＰＯＳＴかＧＥＴかの判定を行い（Ｓ４）、ＧＥＴの場合は、そのリクエストのＨＴＴＰ通信プロトコルのヘッダにクライアントの鍵情報を追加し（Ｓ５）、サーバへ送信する（Ｓ６）。

【００２４】リクエストがＰＯＳＴの場合は、ブラウザから受信した電文にクライアントの電子署名を付け（Ｓ７）、サーバより得たフォームデータ内のサーバ鍵情報を参照し（Ｓ８）、その鍵情報をもとに認証局からサーバ公開鍵証明書を取得し（Ｓ９）、その公開鍵を用いて前記署名付電文を暗号化し（Ｓ１０）、その暗号電文をログ蓄積部に保存し（Ｓ１１）、その後その暗号電文をサーバへ送信する（Ｓ１２）。

【００２５】サーバ１３側の否認防止情報管理装置２１の動作処理手順は図９に示すようになる。まず受信電文がセキュリティ用か否かを調べ（Ｓ１）、セキュリティ用であればその電文、つまりブラウザからのリクエストがＰＯＳＴかＧＥＴの何れであるかを調べ（Ｓ２）、ＧＥＴであれば、その電文のＨＴＴＰヘッダからクライアント鍵情報を取得保存し（Ｓ３）、その電文に対応したコンテンツ又は署名付コンテンツをデータベースから取得し（Ｓ４）、その取得したコンテンツが署名付でなければ（Ｓ５）、そのコンテンツに電子署名を付ける（Ｓ６）。また前記保存したクライアント鍵情報にもとづきクライアントの公開鍵証明書を認証局から取得し（Ｓ７）、その公開鍵を用いて署名付コンテンツを暗号化し（Ｓ８）、その暗号化コンテンツをログ蓄積部に蓄積し（Ｓ９）、その後、その暗号化コンテンツをクライアント端末へ送信する（Ｓ１０）。

【００２６】受信電文がＰＯＳＴであれば、その電文をログ蓄積部に蓄積し（Ｓ１１）、その受信電文を復号化し（Ｓ１２）、また電文中のクライアント鍵情報に基づき認証局からクライアント公開鍵証明書を取得し（Ｓ１

3）、その公開鍵を用いて復号された電文の署名を検証し（Ｓ１４）、その電文がコンテンツの取得要求であればコンテンツデータベースをアクセスし（Ｓ１５）、ステップＳ４へ移る。次にこの発明を電子メールに適用した例を図１０を参照して説明する。メール端末９１とそのメール端末９１が所属するメールサーバ９２との間に否認防止情報管理装置９３が介在され、またメール端末９４とその端末９４が所属するメールサーバ９５との間に否認防止情報管理装置９６が介在される。メール端末９１と否認防止情報管理装置９３間、またメール端末９４と否認防止情報管理装置９５間はそれぞれメール送信プロトコルＳＭＴＰと受信プロトコルＰＯＰで通信が行われ、またメールサーバ９２と否認防止情報管理装置９３間、またメールサーバ９５と否認防止情報管理装置９６間もそれぞれ送信プロトコルＳＭＴＰと受信プロトコルＰＯＰで通信が行われる。メールサーバ９２と９５の間も通信が行われる。

【００２７】例えばメール端末９１から電子メールをメール端末９４へ送信する場合に、メール端末９１よりのメールは否認防止情報管理装置９３に入力される。否認防止情報管理装置９３は図３に示した構成とほぼ同様な構成を備え、安全化判定部３１で安全化条件に該当するかを調べる。例えば通常のアドレスが図１１Ａに示す場合にそのアドレス中の「@」を図１１Ｂに示すように「%」に変更し、かつ最後にキーワード「@ｓｅｃｕｒｉｔｙ」を追加する。この変更はアプリケーションプログラム上で行ってもよいし、メール端末９１内のアドレス帳中の、安全にしたいと思われる相手のアドレスをそのように記述しておく。この場合は、安全化判定部３１で着信アドレス中にキーワード「@ｓｅｃｕｒｉｔｙ」があれば安全化、なければ通常の通信と判定する。安全化の場合は図３中に破線で示す指示により署名部４２で電子署名を付け、その鍵情報（受信側で検証に必要とする公開鍵を得るための情報、つまりＣＡＩＤ、登録アドレス、鍵番号など）を付加し、また受信者の公開鍵証明書を鍵管理アプリケーションプログラムにより認証局装置７１から取得し、その公開鍵により暗号部４３で暗号化してＭＯＳＳのフォーマットでメールサーバ９２へ送る。この際受信アドレスは図１１Ａに示すような通常のアドレスに戻しておく。またメールサーバ９２へ送信すると共にその暗号化メールをログ蓄積部９７に蓄積する。

【００２８】メールサーバ９２はその暗号化メールをメールサーバ９５へ送り、メールサーバ９５はその暗号化メールを否認防止情報管理装置９６へ供給する。否認防止情報管理装置９６も図３に示したものとほぼ同様な構成であり、安全化情報分離部３６でそのＭＯＳＳフォーマットのヘッダのＭＩＭＥ　Ｃｏｎｔｅｎｔ　Ｔｙｐｅから安全化されたものと判断されるとログ蓄積部９８（図１０）に蓄積すると共に復号部３７で復号し、その復号されたメールの署名を検証部３９で検証し、検証に合格するとそのメールをメール端末９４へ送る。検証部３９における送信者の検証用公開鍵の取得は先に述べたと同様な手法による。安全化情報分離部３６で暗号化されたものでないと判断されるとそのままメール端末７４へ送信される。

【００２９】図１１Ｃに示すように、安全化アドレスのキーワード「@ｓｅｃｕｒｉｔｙ」の後に、楕円ＤＨ暗号の相手が使用する秘密鍵番号に対する公開鍵番号と、自分が使用する秘密鍵番号と、自分が署名に用いる鍵番号とを記述しておいてもよい。この例ではこの相手の公開鍵番号の鍵と、自分の秘密鍵とにより共通鍵を生成してアプリケーションデータを暗号化する例である。図１２に示すように安全化して送信したい相手のアドレスとその相手の秘密鍵と対応する公開鍵が登録されている認証局アドレスと、その認証局に登録してある相手のアドレスと、使用する暗号形式と、使用する鍵番号とを組とするリストを作っておき、図３中の安全化条件部１７に格納しておき、送信メール端末から受信したメールのアドレスが安全化条件部１７にあるか否かを安全化判定部３１で判定し、あればその安全化条件部１７のリスト中の該当するアドレスについて格納されている鍵情報を用いて受信者の公開鍵を取得して、暗号部４３で暗号化するようにしてもよい。

【００３０】なお図１１に示した例でアドレス帳を用いる場合は、同一受信者についても、通常アドレスと安全化アドレスとの両者をアドレス帳に記入しておき、その何れかを選択使用できるようにすることもできる。図１０から容易に理解されるように１つのメールサーバ９２に所属する複数のメール端末を１つの否認防止情報管理装置９３により一元的に否認防止情報を管理することもできる。また複数のプロトコルを利用する複数のアプリケーションの一元的に否認防止情報を管理することができる。要はこの発明によれば、後で否認されるおそれのある情報については、その一塊りのアプリケーションデータを署名し、必要に応じて暗号化した状態で、送信情報も、受信情報もログ蓄積部に蓄積しておけばよく、そのアプリケーションデータを作るアプリケーションプログラムには任意のものでもよく、否認防止情報管理装置で送信の際はそのアプリケーションデータが否認されるおそれがあるものであるか否かの判断ができるようにすると共に、受信の際はそれが安全化アプリケーションデータとされたものであるか否かをＭＯＳＳのヘッダのＭＩＭＥ　Ｃｏｎｔｅｎｔ　Ｔｙｐｅなどで区別できればよい。上述では暗号化を公開鍵暗号方式により行ったが、例えばコンテンツを共通鍵で暗号化し、その共通鍵を公開鍵暗号方式により暗号化して同時に送り、受信側で共通鍵を復号し、復号した共通鍵でコンテンツを復号するようにしてもよい。

【００３１】暗号化する場合は、アプリケーションデー

13

タの全体を暗号化し、その暗号化データにヘッダとしてＭＩＭＥ　Ｃｏｎｔｅｎｔ　Ｔｙｐｅと、相手先アドレスを更に付ける。上述の説明から明らかなように否認防止のアプリケーションデータにて必ず署名を付けるが、暗号化はしなくてもよい。

【００３２】

【発明の効果】以上述べたように、この発明によればアプリケーションレベルで一塊りのアプリケーションデータに対し署名を付けてあり、これをこの単位で区別して送信時にも、受信時にもログ蓄積部に蓄積でき、しかもそのデータを思うように改ざんすることはできないため、後でそのようなデータを送ってないとか、受信していないとか、問題が生じた場合にそのログ蓄積部に蓄積されている該当するものを署名検証することにより、当初のデータの正当性を否認することができないことになる。また前記例のように暗号化する場合はその復号のための鍵情報からどこへ送信したかも否認することができなくなる。

【図面の簡単な説明】

【図１】この発明をブラウザとサーバ間の通信に適用した実施例の機能構成を示す図。

【図２】図１で用いられるＧＥＴリクエストデータ１６の例を示す図、Ｂは安全化ＵＲＬリストの例を示す図、Ｃはセキュア用リクエストデータ１８の例を示す図である。

14

る。

【図３】図１中のこの発明による否認防止情報管理装置１５の実施例の機能構成を示す図。

【図４】図１中のこの発明による否認防止情報管理装置２１の実施例の機能構成を示す図。

【図５】この発明をブラウザとサーバ間の通信に適用した他の実施例の機能構成を示す図。

【図６】Ａはサーバより受信したフォームデータ７２の例を示す図、Ｂはリクエストデータ７３の例を示す図、Ｃはセキュア化リクエストデータの例を示す図である。

【図７】図１中のクライアント端末１１をコンピュータにより機能させる場合の機能構成を示す図。

【図８】図３に示した否認防止情報管理装置１５の動作手順の例の一部を示す流れ図。

【図９】図４に示した否認防止情報管理装置２１の動作手順の例の一部を示す流れ図。

【図１０】この発明を電子メールに適用した実施例の機能構成を示す図。

【図１１】Ａは通常アドレス、Ｂ及びＣは安全化アドレスの各例を示す図である。

【図１２】安全化アドレスリストの例を示す図。

【図１３】従来のクライアントとサーバ間の暗号化通信を説明するための図。

【図１】

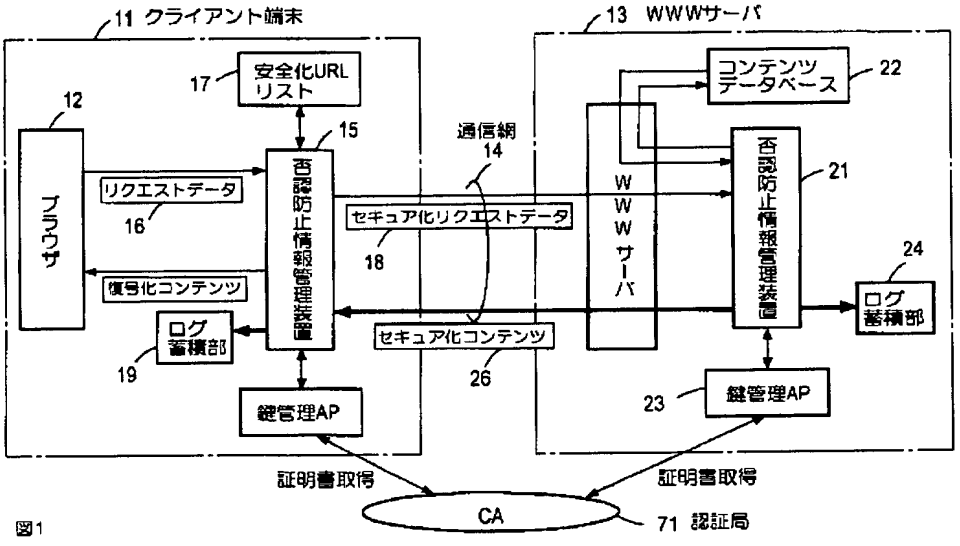


図1

【図２】

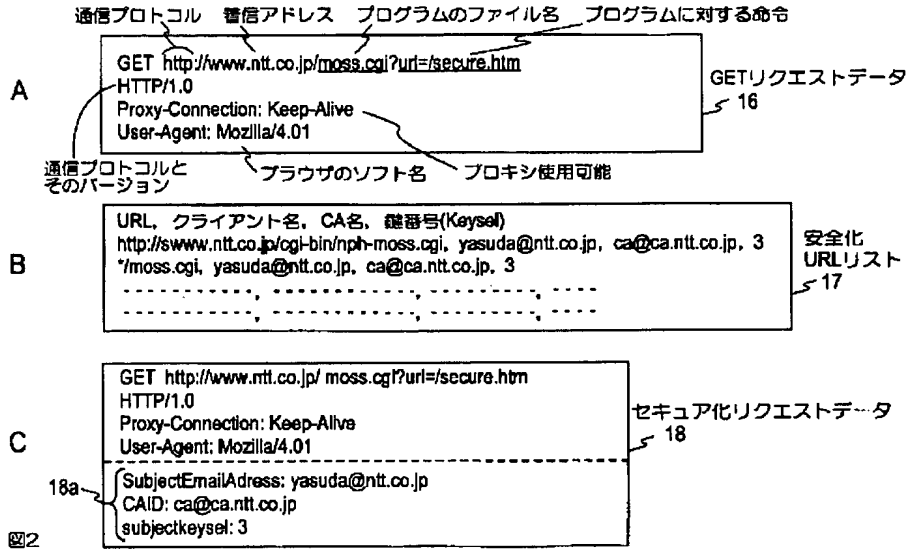


図2

【図３】

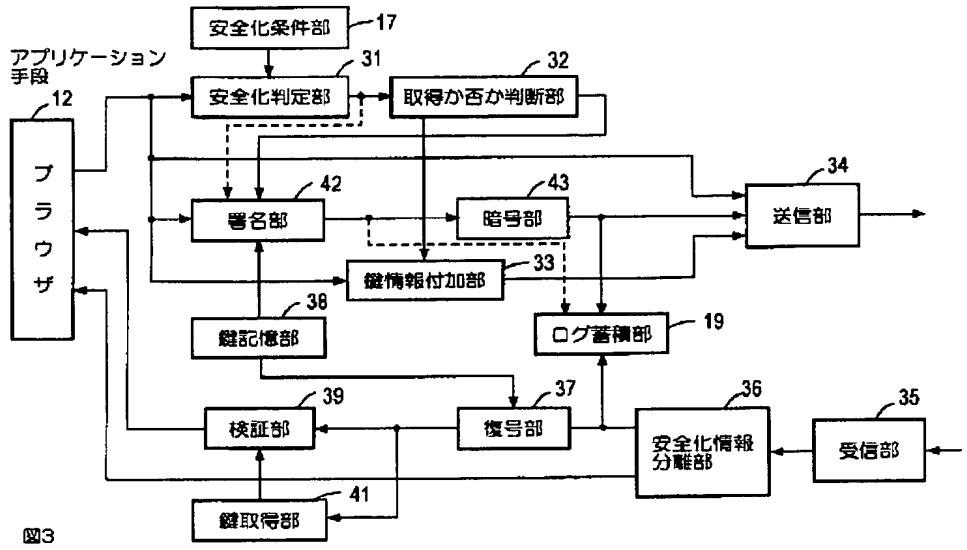


図3

【図１１】

通常アドレス	yasuda@ntt.co.jp
安全化アドレス	yasuda% ntt.co.jp@security
〃	yasuda% ntt.co.jp@security [相手DHkeysel[自分DHKeysel[自名EsignKeysel]]]

図11

【図１２】

アドレス	認証局アドレス	登録アドレス	暗号形式	鍵番号
yasuda@winca	ca@winca	yasuda@winca	E-DH256	4
ogihara@winca	ca@winca	ogihara@winca	E-DH256	6
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

図12

【図４】

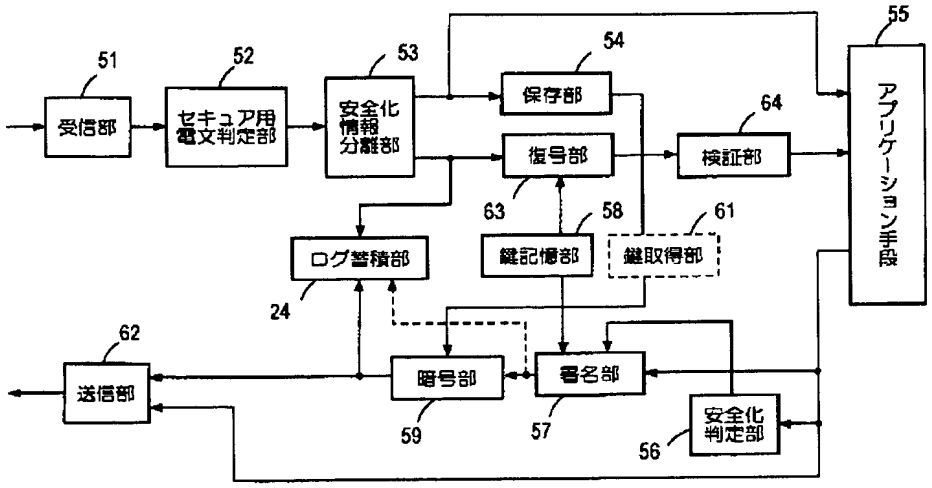


図4

【図５】

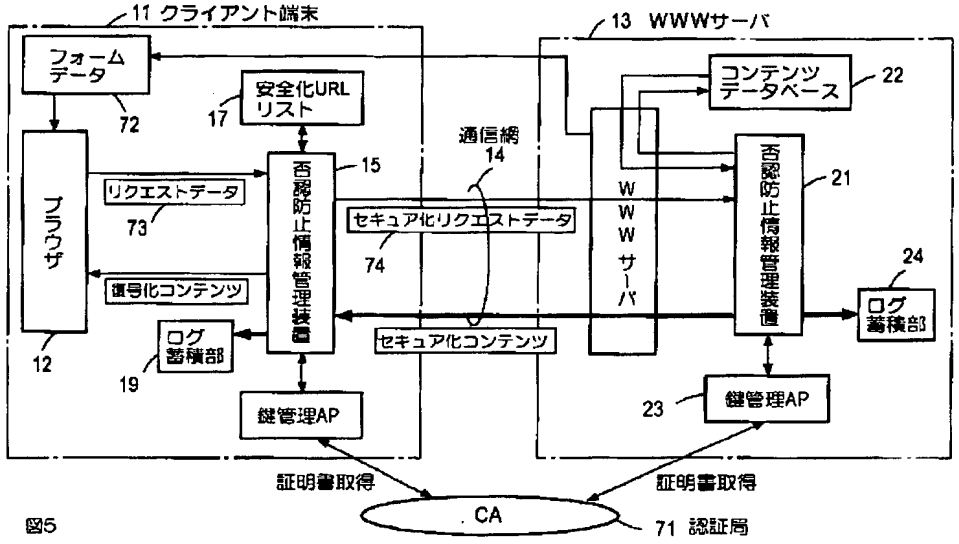


図5

【図１３】

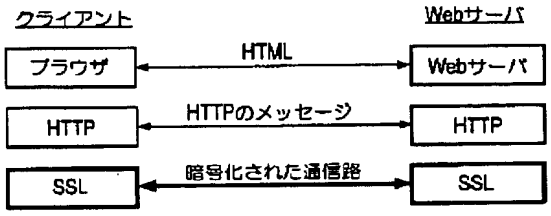


図13

【図６】

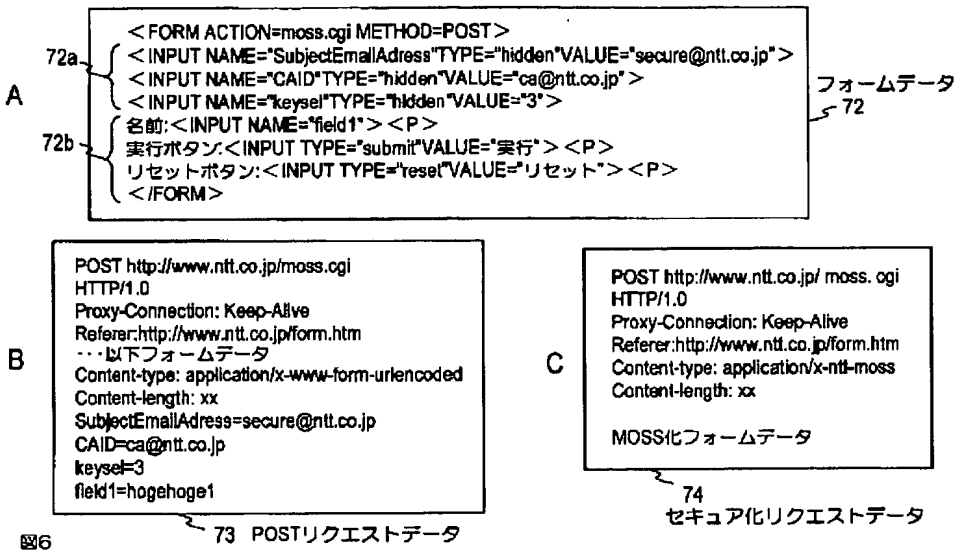

A
72a
72b
＜FORM ACTION=moss.cgi METHOD=POST＞
＜INPUT NAME="SubjectEmailAdress"TYPE="hidden"VALUE="secure@ntt.co.jp"＞
＜INPUT NAME="CAID"TYPE="hidden"VALUE="ca@ntt.co.jp"＞
＜INPUT NAME="keysel"TYPE="hidden"VALUE="3"＞
名前:＜INPUT NAME="field1"＞＜P＞
実行ボタン:＜INPUT TYPE="submit"VALUE="実行"＞＜P＞
リセットボタン:＜INPUT TYPE="reset"VALUE="リセット"＞＜P＞
＜/FORM＞
フォームデータ
72
B
POST http://www.ntt.co.jp/moss.cgi
HTTP/1.0
Proxy-Connection: Keep-Alive
Referer:http://www.ntt.co.jp/form.htm
・・・以下フォームデータ
Content-type: application/x-www-form-urlencoded
Content-length: xx
SubjectEmailAdress=secure@ntt.co.jp
CAID=ca@ntt.co.jp
keysel=3
field1=hogehoge1
73 POSTリクエストデータ
C
POST http://www.ntt.co.jp/ moss. cgi
HTTP/1.0
Proxy-Connection: Keep-Alive
Referer:http://www.ntt.co.jp/form.htm
Content-type: application/x-ntt-moss
Content-length: xx
MOSS化フォームデータ
74
セキュア化リクエストデータ

図6

【図７】

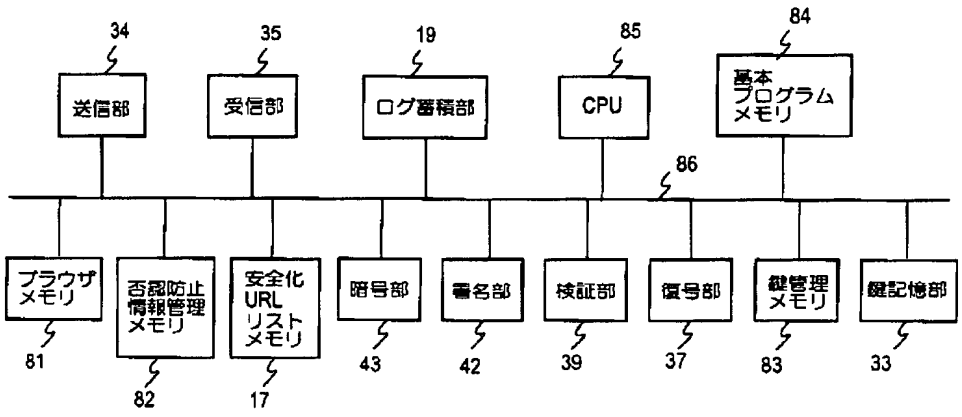

34
35
19
85
84
送信部
受信部
ログ蓄積部
CPU
基本プログラムメモリ
86
ブラウザメモリ
否認防止情報管理メモリ
安全化URLリストメモリ
暗号部
署名部
検証部
復号部
鍵管理メモリ
鍵記憶部
81
82
17
43
42
39
37
83
33

図7

【図８】

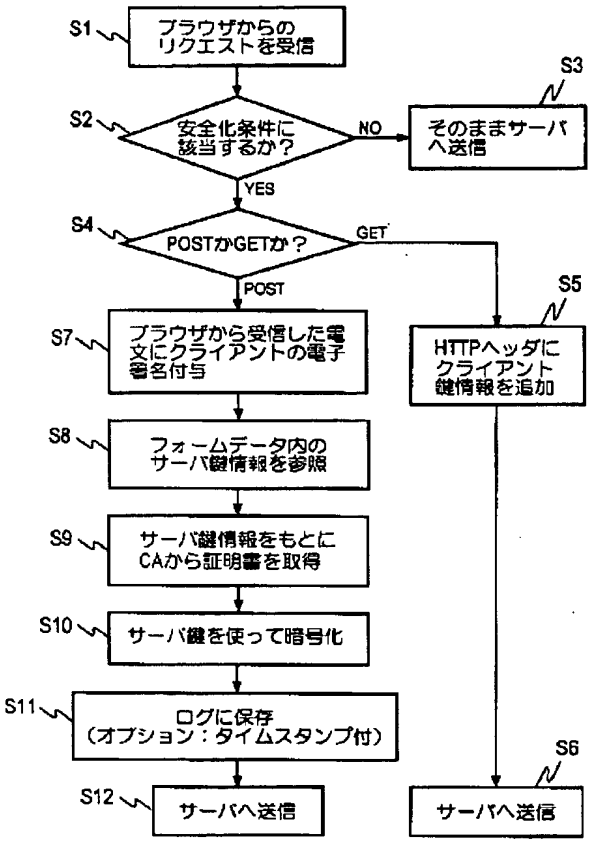


図8

【図９】

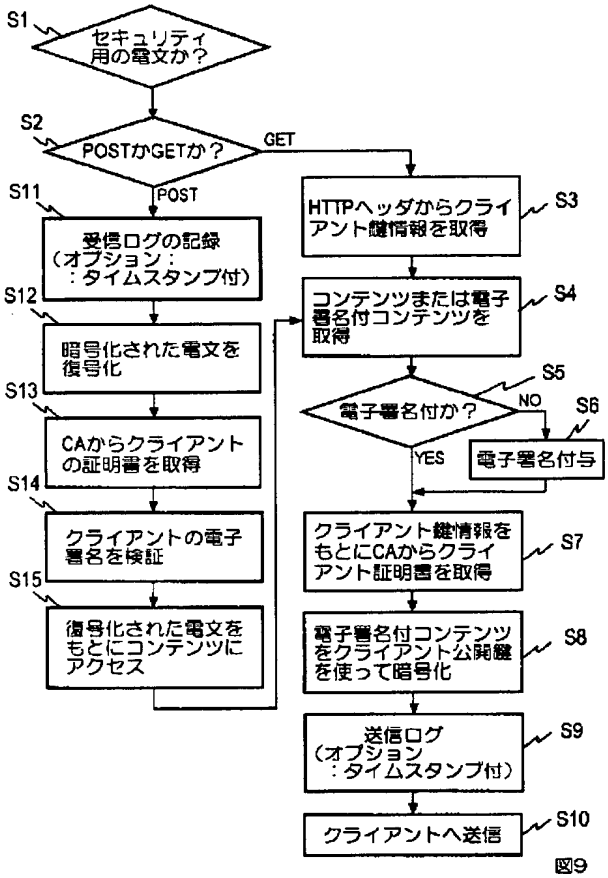


図9

【図１０】

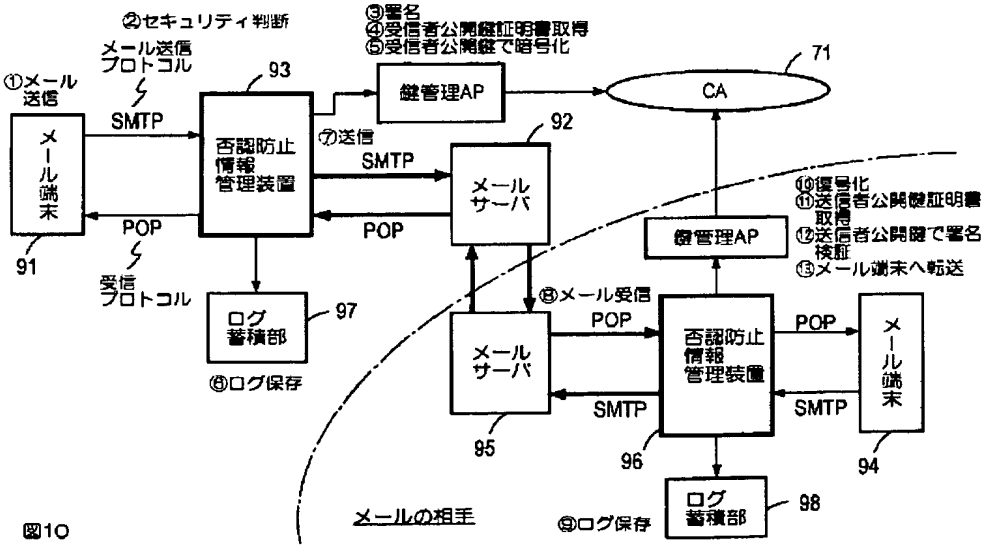


図10

フロントページの続き

(72)発明者　渡辺　徹
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　荻原　利彦
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　田渕　博康
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

Ｆターム(参考)　5B017 AA08 BA07 CA16
5B085 AC14 AE13 AE29 BG07
5J104 AA09 LA03 LA06 MA02 NA02
PA08 PA09